

Foto: IBM Q

Kvantové počítače: revoluce nebo slepá ulička?



Univerzita Palackého
v Olomouci

Karel Lemr

Společná laboratoř Optiky,
Univerzita Palackého v Olomouci

web: <http://jointlab.upol.cz/lemr>,

email: k.lemr@upol.cz



Ze světového tisku ...

OUT THERE?

Quantum Computing Is Coming, Bit by Qubit

With transmons and entanglement, scientists strive to put subatomic weirdness to work on the human scale.



NEWS

[Home](#)[Video](#)[World](#)[UK](#)[Business](#)[Tech](#)[Science](#)[Stories](#)[Entertainment & Arts](#)Science & Environment

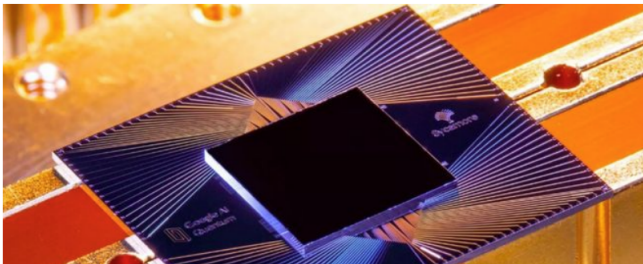
Google claims 'quantum supremacy' for computer

By Paul Rincon
Science editor, BBC News website

🕒 23 October 2019 📄



🔗 Share

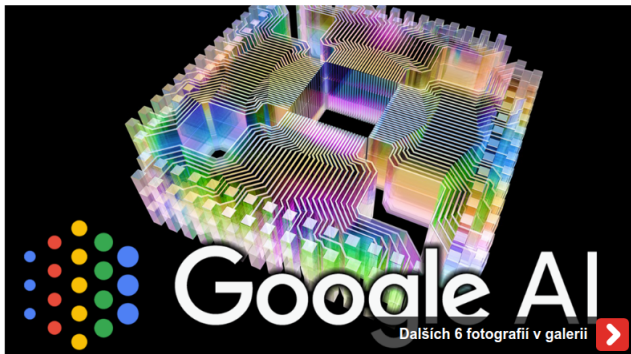


Přišla doba kvantová? Google tvrdí, že dnešní počítače jsou překonány

28. října 2019



Tým společnosti Google tvrdí, že zcela nový typ počítačů – kvantové – v některých ohledech nenávratně překonal počítače klasické. Patrně je to pravda, a to i přesto, že kvantové počítače jsou v plenkách a výzkumný kolektiv Googlu se v práci splete o bezmála deset tisíc let.



27. ŘÍJNA 2019 10:14 | [LIDOVKY.CZ](#) > [RELAX](#) > [VĚDA](#)

Vědci údajně dosáhli kvantové nadřazenosti. Jejich ultrarychlý může změnit svět



GOOGLE OD BŘEZNA TAJIL BEZPEČNOSTNÍ CHYBU NA SVĚ SOCIÁLNÍ SÍTI GOOGLE +. |
FOTO: AP



Vědci zjistili,
3000 lety pil
lahviček



Co je to kvantový počítač?

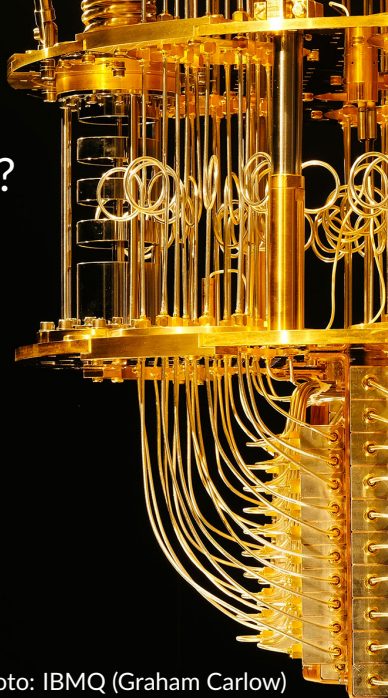


Foto: IBMQ (Graham Carlow)

Co je to kvantový počítač?

Co je na něm
vlastně kvantového?

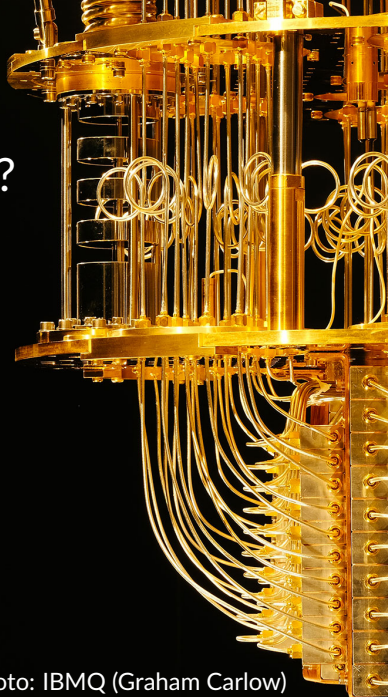


Foto: IBMQ (Graham Carlow)

Co je to kvantový počítač?

Co je na něm
vlastně kvantového?

Je opravdu tak úžasný?

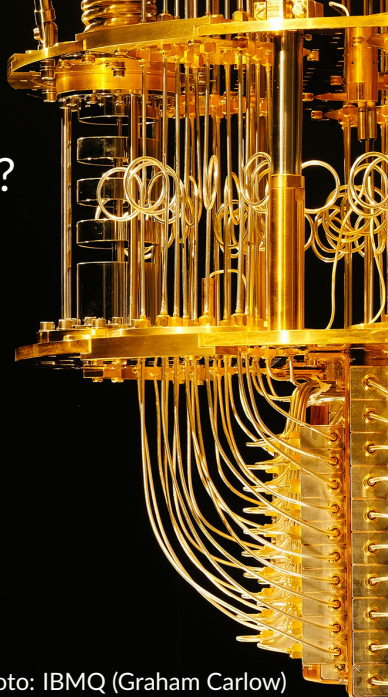


Foto: IBMQ (Graham Carlow)

Kvantová fyzika v 5 minutách

Volksstimme

Sozialdemokratisches Organ für Magdeburg und Umgegend.

Die Volksstimme erscheint täglich abends mit Ausnahme der Sonn- und Festtage mit dem Datum des folgenden Tages. — Gewerkschaftliche Redaktionen mit Ausnahme der Zeitschriften: Richard Ritzsch, Magdeburg. Verantwortlich: Dr. Heinrich Wagner, Berlin. Verlag von Hermann Göttsch, Magdeburg. Druck von Hermann Göttsch, Magdeburg. Geschäftsstelle: Jakobstraße 44, Fernsprecher 1587. Redaktions-Druck: Magdeburger 8, Fernsprecher 161.

Beitragende zahlbaren Abonnementspreis: Vierteljährlich (inkl. Frachtkosten) 2 Mk. 25 Pf., monatlich 80 Pf. Der Preis kann in Vorauszahlungen monatlich 1 Viertel, 170 Pf., 2 Viertel, 340 Pf., an der Expedition und den Verkaufsstellen vorbezahlt werden. Einzelne Nummern 20 Pf. Bei den Volksstimmen 250 gibt. Beilagen: Einzelne Nummern (einmal) der Monatsbeilage, sowie der Wochenbeilage Die Neue Welt 10 Pf. Sonderausgaben die halbjährliche Beilage 15 Pf. Halb-Jahreshefte der 1928

Nr. 291.

Magdeburg, Freitag, den 14. Dezember 1900.

II. Jahrgang.

Die heutige Nummer umfasst 8 Seiten.

Der Etat-Debatte dritter Tag.

Unser parlamentarischer hg.-Korrespondent schreibt uns: Der dritte Tag der Etats-Beratung stand vollständig unter dem Zeichen der Buren resp. des Nichtempfanges des dem Präsidenten Krüger, sowie unter dem Zeichen der 12000 Mart-Affaire aus dem Reichsamt des Innern. Das letztere ist für die politischen Zustände Deutschlands außerordentlich bezeichnend: Die wichtigste Frage der inneren Politik, die Frage der Getreidezölle, muß zurücktreten, die nach der Reichstag sich mit Dingen beschäftigen muß, die wohl den eigenen Erklärungen des Reichskanzlers durchaus geeignet erscheinen, die Regierung der einseitigen Parteinahme gegen die Arbeiter zu beschuldigen.

Der Anfang der Verhandlungen ließ freilich die lebhafteste Debatte, die sich nachher entspann, noch nicht erwarten. Bemerkenswert ist nur die Tatsache, daß Herr Rickert im Namen der freisinnigen Vereinigung dem Reichskanzler für die Abweisung Krügers dankte; bei diesen Wobelschlämpen geht die Verneinung nach oben so weit, daß sie dem Empfinden des gesamten Volkes zum Trotz die Handlungen der Regierung billigen. Das wird so lange dauern, bis das Volk ihnen die Gelegenheit zu dieser Vertierung der Volksinteressen gänglich nimmt.

Als aber der Deutsche Haff, soeben aus dem Gang von dem Präsidenten Krüger zurückgekehrt, die Tribüne betrat, kam die Transvaal-Angelegenheit sofort

öffentlichen Arbeiten in einem neuerlichen Erlaß an den Vorstand der Baugeschäfte Verlin für „nicht mit dem staatlichen Interesse vereinbar“. Der Minister will von Fall zu Fall entscheiden, ob bei Streiks der Unternehmer von vertraglichen Verpflichtungen entbunden werden kann. Die Behörden sollen jedoch an der bisherigen Praxis festhalten und den durch unverschuldete Arbeitskämpfe hervorgerufenen besonderen Verhältnissen bei Beurteilung der dem Unternehmer vorliegenden Verpflichtungen in gleich wohlwollender Weise ausreichend Rechnung tragen, wie dies bisher geschehen ist.

— Daß der neue Handelsvertragsverein auch fernerhin die Frage der Erhöhung der Getreidezölle ungelöst läßt, ergibt sich nach der freisinnigen Zeitung aus der Nr. 1 der von seinem Generalsekretär versandten Korrespondenz. In derselben werden die Handelskammern aufgefordert, gegen den Doppeltarif und für die Erneuerung der Handelsverträge bei den Landesregierungen zu petitionieren. Mit seiner Seite ist aber davon die Rede, daß dieselben die Erhöhung der Lebensmittelpreise zu bekämpfen haben. Und einem solchen Verein haben Optimisten schon die Bezeichnung Anti-Kornzoll-Liga gegeben!

— Die Antifeministen Dühringhieser Richtung wollen von dem Grafen Bülker nichts wissen. In ihrem Organ „Der Personalität und Expansionist“ wird dem Grafen Bülker plumper, aller Gattung bärer Geblänsch, dem man die Effetation und künstliche Genachtheit sofort ansieht, vorgeworfen und über die Belleid, die Juden weg setzen

Proklamationen des Lord Roberts und erklärt, die Regierung wünsche das Ende des Geraillakrieges. Wenn im Geiste dieser Proklamationen Abmachungen getroffen werden könnten, die den zur Uebergabe aufgeforderten Buren mehr Vertrauen einflößen, so würde die Regierung gern die nötigen Bestimmungen treffen; Vorbedingung hierfür sei aber, daß diese Abmachungen nicht als Beweis von Schwäche ausgelegt würden und dann eine Verlängerung des Kampfes herbeiführen. —

Ungarn.

Dem Fürsten Ferdinand ist es gelungen, ein neues Kabinett zusammenzukommen. Da damit die inneren Wären aber nicht beseitigt sind, ist zur Abwechslung einmal wieder die Sozianse aufgelöst worden. Die Remonaffen sollen am 28. Januar alten Stils stattfinden. —

Serbien.

Der frühere Minister Gentschitsch wurde wegen Majestätsbeleidigung und öffentlicher Beleidigung der Regierung zu sieben Jahren einfachen Gefängnisses verurteilt.

Südafrika.

Wie aus Holland gemeldet wird, hat die deutsche Regierung aus Gründen der niederländischen Regierung den deutschen Konsul in Laurens Marquis mit dem Wahrgenahme der niederländischen Interessen beauftragt. Das Amsterdamer Amisblatt bestätigt diese Meldung. —

China.

Volksstimme

Sozialdemokratisches Organ für Westfalen und Rheinland

Die Volksstimme
erschienen
am 14. d. M.
Nr. 21

14. Dezember 1900.

Wg. von den
Anzeigen
verlegt, Louis der
Mühlh. Nr. 128
gang.

Die heutige Nummer umfasst 5 Seiten.

Der Etat-Debatte dritter Tag.

Unser parlamentarischer hg.-Korrespondent schreibt uns: Der dritte Tag der Etats-Beratung stand vollständig unter dem Zeichen der Buren resp. des Nichtempfanges des dem Präsidenten Krüger, sowie unter dem Zeichen der 12000 Mark-Affaire aus dem Reichsamt des Innern. Das letztere ist für die politischen Zustände Deutschlands außerordentlich bezeichnend: Die wichtige Frage der inneren Politik, die Frage der Getreidezölle, muß zurücktreten, weil der Reichstag sich mit Dingen beschäftigen muß, die nach den eigenen Erklärungen des Reichskanzlers durchaus geeignet erscheinen, die Regierung der einseitigen Parteinahme gegen die Arbeiter zu beschuldigen.

Der Anfang der Verhandlungen ließ freilich die lebhafteste Debatte, die sich nachher entspann, noch nicht erwarten. Bemerkenswert ist nur die Thatsache, daß Herr Rickert in Namen der freisinnigen Vereinigung dem Reichskanzler für die Abweisung Krügers dankte; bei diesen Wobelschlämpereien geht die Verneinung nach oben so weit, daß sie dem Empfinden des gesamten Volkes zum Trost die Handlungen der Regierung billigen. Das wird so lange dauern, bis das Volk ihnen die Gelegenheit zu dieser Vertierung der Volksinteressen gänglich nimmt.

Als aber der Deutsche Botschafter, soeben aus dem Gang von dem Präsidenten Krüger zurückgekehrt, die Tribüne betrat, kam die Transvaal-Angelegenheit sofort

openamente in einen neuerlichen Ersatz an den Vorstand der Bangehäute Verlin für „nicht mit dem staatlichen Interesse vereinbar“. Der Minister will von Fall zu Fall entscheiden, ob bei Streiks der Unternehmer von vertraglichen Verpflichtungen entbunden werden kann. Die Behörden sollen jedoch an der seitherigen Praxis festhalten und den durch unverschuldete Arbeitskämpfe hervorgerufenen besonderen Verhältnissen bei Beurteilung der dem Unternehmer vorliegenden Verpflichtungen in gleich wohlwollender Weise ausreichende Rechnung tragen, wie dies bisher geschehen ist.

— Daß der neue Handelsvertragsverein auch fernerhin die Frage der Erhöhung der Getreidezölle ungehen will, ergibt sich nach der Freitagigen Zeitung aus der Nr. 1 der von seinem Generalsekretär versandten Korrespondenz. In derselben werden die Handelskammern aufgefordert, gegen den Doppeltarif und für die Erneuerung der Handelsverträge bei den Landesregierungen zu petitionieren. Mit keiner Silbe ist aber davon die Rede, daß dieselben die Erhöhung der Lebensmittelpreise zu bekämpfen haben. Und einem solchen Verein haben Optimisten schon die Bezeichnung Anti-Kornzoll-Liga gegeben!

— Die Antifeministen Dühringischer Richtung wollen von dem Grafen Büdler nichts wissen. In ihrem Organ „Der Personalität und Emancipator“ wird dem Grafen Bilder plumper, aller Gattung borer Gebrauchs, dem man die Effetation und künstliche Genachtheit sofort ansieht, vorgeworfen und über die Belleid, die Juden weg setzen

Proklamationen des Lord Roberts und erklärt, die Regierung wünsche das Ende des Ostafrikakrieges. Wenn im Geiste dieser Proklamationen Abmachungen getroffen werden könnten, die den zur Uebergabe aufgeforderten Buren mehr Vertrauen einflößen, so würde die Regierung gern die nötigen Bestimmungen treffen; Vorbedingung hierfür sei aber, daß diese Abmachungen nicht als Beweis von Schwäche ausgelegt würden und dann eine Verlängerung des Kampfes herbeiführen. —

Ungarn.

Dem Fürsten Ferdinand ist es gelungen, ein neues Kabinett zusammenzutrommeln. Da damit die inneren Wirren aber nicht beendet sind, ist zur Abwechslung einmal wieder die Sozianke aufgelöst worden. Die Remonstren sollen am 28. Januar alten Stils stattfinden. —

Serbien.

Der frühere Minister Gentschitsch wurde wegen Majestätsbeleidigung und öffentlicher Gefährdung der Regierung zu sieben Jahren einfachen Gefängnisses verurteilt.

Südafrika.

Wie aus Holland gemeldet wird, hat die deutsche Regierung auf Ersuchen der niederländischen Regierung den deutschen Konsul in Durango Marques mit dem Auftrage beauftragt, die niederländischen Interessen zu beschützen. Das Amsterdamer Amisblatt bestätigt diese Meldung. —

China.



schon Gesellschaft

Lehr, später O. Lember

vom 14. Dezember 1900

Schriftführer: H. du Bois

Name des Vortragenden

Gegenstand des Vortrages

Hr. M. Planck

Hr. H. Diepelt

Der Vers. theilt das Ableben eines unserer anwesenden Mitglieder mit:

Hr. Prof. A. Oberbeck (Nachruf später)

Hr. Prof. E. Rotteler (geb. 18-4-36)

{Hauptarbeiten: optik, aberration, Dispersion}

Die Mitglieder erheben sich von ihren Plätzen.

1. Ueber das sog. Wien'sche Paradoxon.

2. Ueber Theorie der Gesetze der Energievertheilung im Normalspektrum.

Ueber die bisherigen Bestimmungen der Wärmeleitung

Zu Mitgliedern wurden gewählt

Herr Dr. E. Grünstein

Dr. F. Dolzalek

Dr. F. Bräutigam

Ausgeschieden

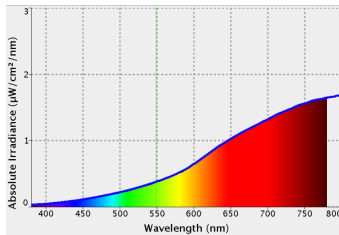
Anderweitige Beschlüsse und Mittheilungen

Zu Mitgliedern wurden vorgeschlagen

Herr Prof. Dr. Mücke durch Rubens

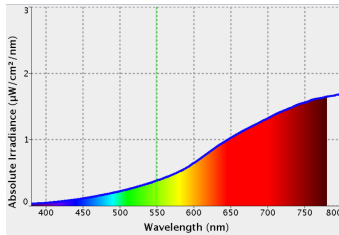
Revoluční teorie jako akt zoufalství

- Planck odvodil tvar **spektra černého tělesa**
- *černé těleso vyzařuje jen díky své teplotě:
Slunce, žárovka*



Revoluční teorie jako akt zoufalství

- Planck odvodil tvar **spektra černého tělesa**
- *černé těleso vyzařuje jen díky své teplotě:
Slunce, žárovka*
- *jako akt zoufalství* použil hypotézu:
**výměna energie mezi elektromagnetickým
polem a látkou probíhá po dávkách
(kvantech)**
- položil základy **KVANTOVÉ FYZIKY**

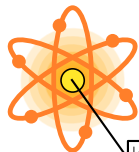


Handwritten mathematical derivations in quantum mechanics, likely related to the harmonic oscillator. The equations include:

$$\hat{Q}_H^+ |00\rangle = \hat{a}_H^+ \hat{Q}_H^+ |00\rangle = \left(\frac{1}{\sqrt{2}} \hat{H}_a \hat{H}_b \right)$$
$$\hat{Q}_V^+ |00\rangle = \hat{q}_V^+ \left(\frac{1}{\sqrt{2}} \hat{L}_V^+ + i \sqrt{\frac{2}{3}} \hat{a}_V \right) |00\rangle$$
$$|q\rangle = \left(\frac{1}{\sqrt{2}} |V\rangle + \sqrt{\frac{2}{3}} i |V_a\rangle \right) = \left(\frac{1}{\sqrt{2}} |H_V\rangle + \dots \right)$$



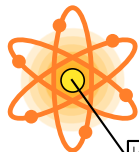
V kvantovém světě ...



$$|\Psi\rangle : \{x, y, z\}$$

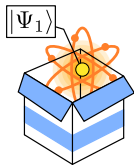
kvantový stav popisuje vlastnosti objektu
například: vektor polohy nebo rychlosti

V kvantovém světě ...



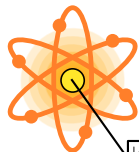
$$|\Psi\rangle : \{x, y, z\}$$

kvantový stav popisuje vlastnosti objektu
například: vektor polohy nebo rychlosti



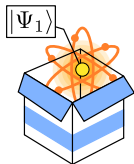
je-li platný jeden stav (*částice je v modré krabici*)

V kvantovém světě ...



$$|\Psi\rangle : \{x, y, z\}$$

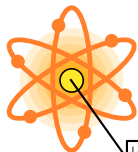
kvantový stav popisuje vlastnosti objektu
například: vektor polohy nebo rychlosti



je-li platný jeden stav (částice je v *modré* krabici)
a zároveň druhý stav (částice je v *zelené* krabici)

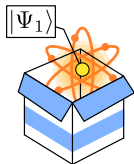


V kvantovém světě ...

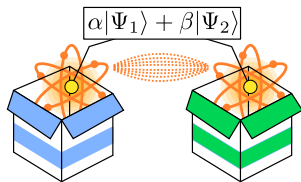


$$|\Psi\rangle : \{x, y, z\}$$

kvantový stav popisuje vlastnosti objektu
například: vektor polohy nebo rychlosti

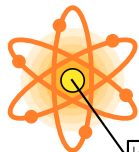


je-li platný jeden stav (částice je v *modré* krabici)
a zároveň druhý stav (částice je v *zelené* krabici)



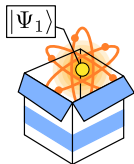
pak se částice může nacházet **v obou stavech naráz** (*princip superpozice*)

V kvantovém světě ...

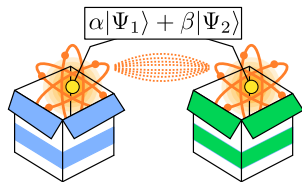


$$|\Psi\rangle : \{x, y, z\}$$

kvantový stav popisuje vlastnosti objektu
například: vektor polohy nebo rychlosti



je-li platný jeden stav (částice je v *modré* krabici)
a zároveň druhý stav (částice je v *zelené* krabici)

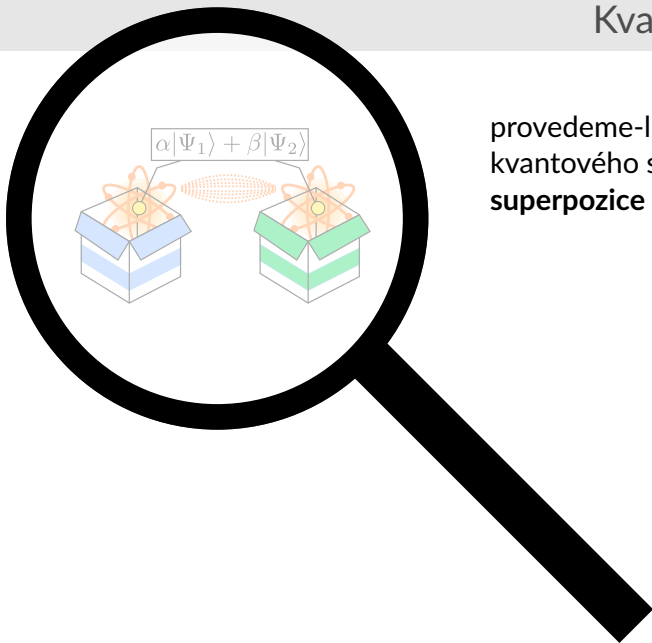


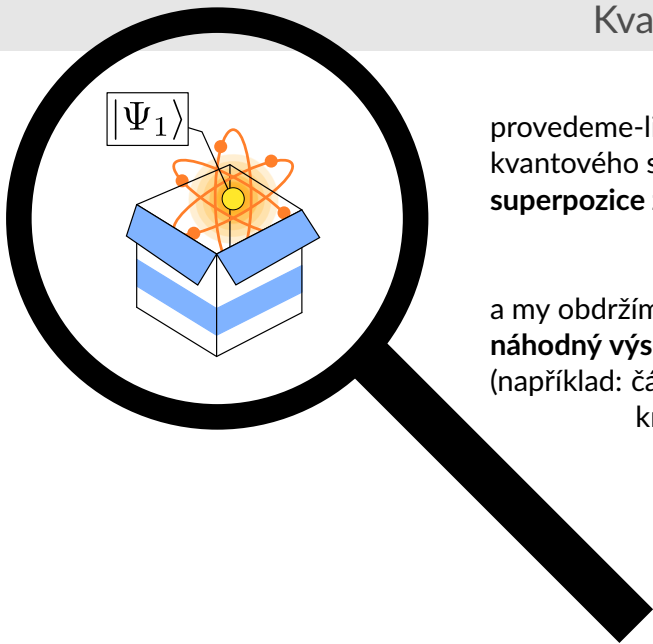
$$\alpha|\Psi_1\rangle + \beta|\Psi_2\rangle$$

pak se částice může nacházet **v obou stavech naráz** (*princip superpozice*)

a to ještě s různými vahami!

provedeme-li pozorování
kvantového stavu,
superpozice zkolabuje



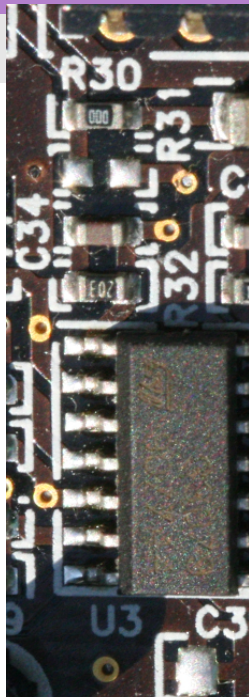


provedeme-li pozorování
kvantového stavu,
superpozice zkolabuje

a my obdržíme
náhodný výsledek
(například: částice je v modré
krabici)

Jak to ale souvisí s počítáním?

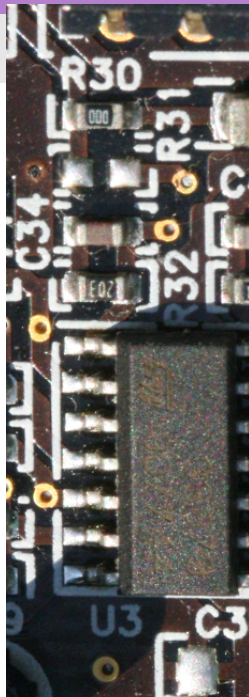
Klasické počítání



Zápis informace:



bity 0, nebo 1



Zápis informace:

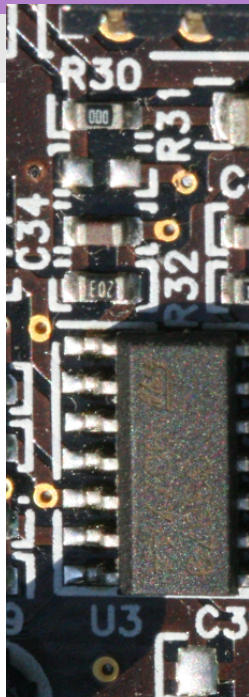


bity 0, nebo 1

Zpracování informace:



klasická fyzika (informatika)



Klasické počítání

Zápis informace:



bity 0, nebo 1

Zpracování informace:

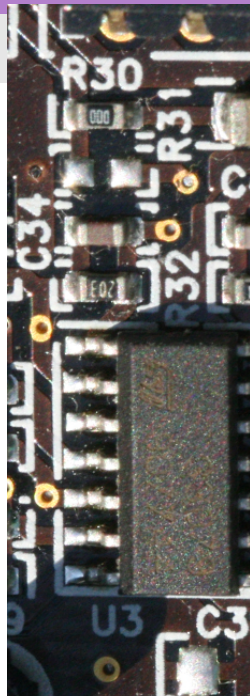


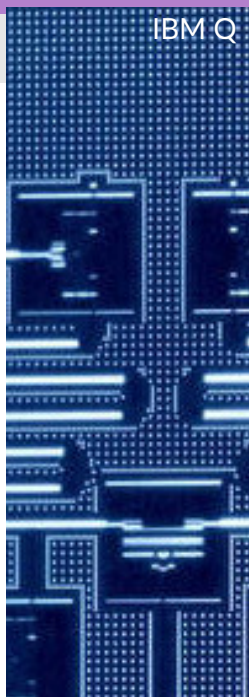
klasická fyzika (informatika)

- všechny algoritmy lze implementovat s tužkou a papírem
- klasická teorie elektromagnetického pole je stará více než 150 let



Foto: Wikipedia

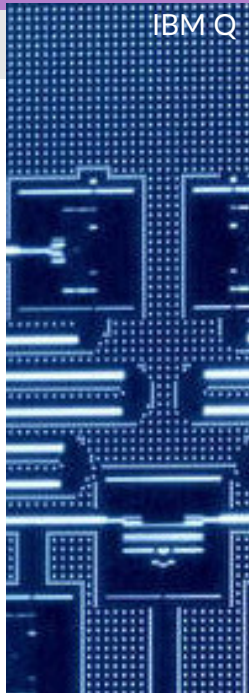




Zápis informace:



qubity $|0\rangle$, $|1\rangle$ a jejich superpozice



Zápis informace:

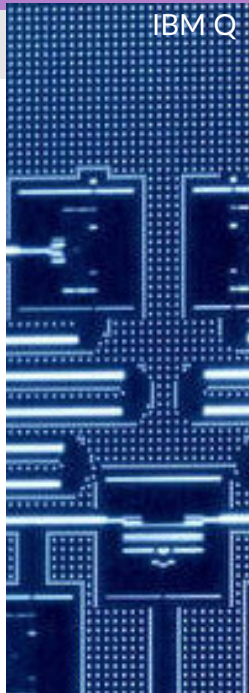


qubity $|0\rangle$, $|1\rangle$ a jejich superpozice

Zpracování informace:



kvantová fyzika



Zápis informace:



qubity $|0\rangle$, $|1\rangle$ a jejich superpozice

Zpracování informace:



kvantová fyzika

- princip superpozice: $0,01110\dots|0\rangle + 0,11101\dots|1\rangle$
(1 qubit nese teoreticky nekonečné množství klasické informace)

Zápis informace:



qubity $|0\rangle$, $|1\rangle$ a jejich superpozice

Zpracování informace:



kvantová fyzika

- princip superpozice: $0,01110\dots|0\rangle + 0,11101\dots|1\rangle$
(1 qubit nese teoreticky nekonečné množství klasické informace)
- při měření superpozice kolabuje:
z 1 qubitu vyčteme pouze 1 bit

Historické milníky



- **Stephen Wiesner** navrhuje použít kvantové stavy jako nositele informace



Foto: Wikipedia

- **Stephen Wiesner** navrhuje použít kvantové stavy jako nositele informace
- představuje koncept kvantových bankovek

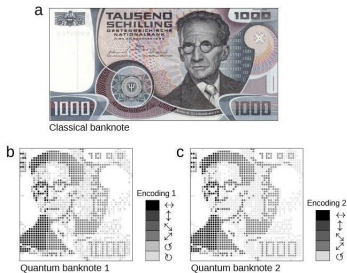
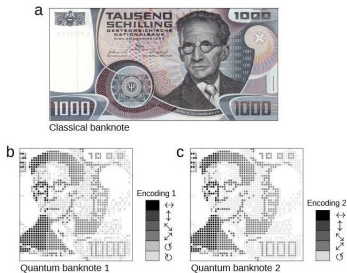


Foto: Wikipedia

- **Stephen Wiesner** navrhuje použít kvantové stavy jako nositele informace
- představuje koncept kvantových bankovek



- na tehdejší dobu nepraktický



Foto: Wikipedia

- rozvoj teoretických poznatků

- rozvoj teoretických poznatků
- 1976: **Roman Stanisław Ingarden** publikuje práci *Quantum Information Theory*

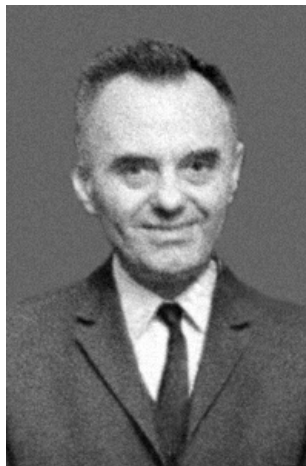


Foto: Wikipedia

- rozvoj teoretických poznatků
- 1976: **Roman Stanisław Ingarden** publikuje práci *Quantum Information Theory*
- 1980: **Paul Benioff** popíše počítač pomocí kvantové mechaniky



Foto: Wikipedia

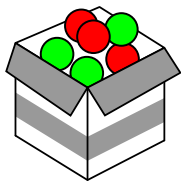
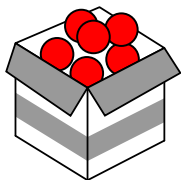
- rozvoj teoretických poznatků
- 1976: **Roman Stanisław Ingarden** publikuje práci *Quantum Information Theory*
- 1980: **Paul Benioff** popíše počítač pomocí kvantové mechaniky
- 1985: **David Deutsch** definuje univerzální kvantový počítač



Foto: osobní web

- teoretici dokazují hmatatelné výhody kvantového počítání

- teoretici dokazují hmatatelné výhody kvantového počítání
- 1992: **David Deutsch a Richard Jozsa** představují první algoritmus, kde kvantový počítač dosahuje zrychlení



klasicky: počet pokusů roste s N
kvantově: 1 souhrnné měření

- teoretici dokazují hmatatelné výhody kvantového počítání
- 1992: **David Deutsch a Richard Jozsa** představují první algoritmus, kde kvantový počítač dosahuje zrychlení
- 1994: **Peter Shor** publikuje kvantový algoritmus pro faktORIZACI součinu prvočísel

$$7 \times 13 =$$

- teoretici dokazují hmatatelné výhody kvantového počítání
- 1992: **David Deutsch a Richard Jozsa** představují první algoritmus, kde kvantový počítač dosahuje zrychlení
- 1994: **Peter Shor** publikuje kvantový algoritmus pro faktORIZACI součinu prvočísel

$$7 \times 13 = 91$$

- teoretici dokazují hmatatelné výhody kvantového počítání
- 1992: **David Deutsch a Richard Jozsa** představují první algoritmus, kde kvantový počítač dosahuje zrychlení
- 1994: **Peter Shor** publikuje kvantový algoritmus pro faktORIZACI součinu prvočísel

$$7 \times 13 = 91$$

$$35 =$$

- teoretici dokazují hmatatelné výhody kvantového počítání
- 1992: **David Deutsch a Richard Jozsa** představují první algoritmus, kde kvantový počítač dosahuje zrychlení
- 1994: **Peter Shor** publikuje kvantový algoritmus pro faktORIZACI součinu prvočísel

$$7 \times 13 = 91$$

$$35 = 5 \times 7$$

- teoretici dokazují hmatatelné výhody kvantového počítání
- 1992: **David Deutsch a Richard Jozsa** představují první algoritmus, kde kvantový počítač dosahuje zrychlení
- 1994: **Peter Shor** publikuje kvantový algoritmus pro faktORIZACI součinu prvočísel

$$7 \times 13 = 91$$

$$35 = 5 \times 7$$

$$437 =$$

- teoretici dokazují hmatatelné výhody kvantového počítání
- 1992: **David Deutsch a Richard Jozsa** představují první algoritmus, kde kvantový počítač dosahuje zrychlení
- 1994: **Peter Shor** publikuje kvantový algoritmus pro faktORIZACI součinu prvočísel

$$7 \times 13 = 91$$

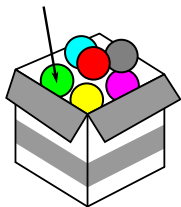
$$35 = 5 \times 7$$

$$437 = 19 \times 23$$

klasicky: $\exp(N)$,
N ... délka čísel

kvantově: $\text{poly}(N)$

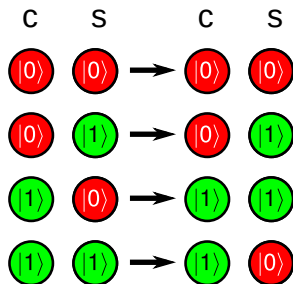
- teoretici dokazují hmatatelné výhody kvantového počítání
- 1992: **David Deutsch a Richard Jozsa** představují první algoritmus, kde kvantový počítač dosahuje zrychlení
- 1994: **Peter Shor** publikuje kvantový algoritmus pro faktORIZACI součinu prvočísel
- 1996: **Lov Grover** nachází kvantový algoritmus pro vyhledání v neuspořádané databázi



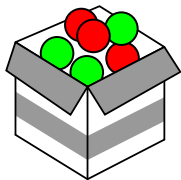
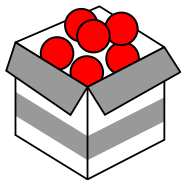
klasicky: počet pokusů roste s N
kvantově: roste s $\sqrt{N}$

- experimentátoři zkouší první krůčky

- experimentátoři zkouší první krůčky
- 1995: **Christopher Monroe a David Wineland** implementují první logické hradlo pro kvantový počítač



- experimentátoři zkouší první krůčky
- 1995: **Christopher Monroe a David Wineland** implementují první logické hradlo pro kvantový počítač
- 1998: **Jonathan A. Jones a Michele Mosca** implementují Deutschův-Jozsovův algoritmus (2 qubity)

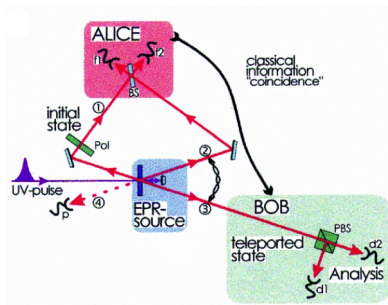


klasicky: roste s N

kvantově: 1 souhrnné měření

90. léta 20. století

- experimentátoři zkouší první krůčky
- 1995: **Christopher Monroe a David Wineland** implementují první logické hradlo pro kvantový počítač
- 1998: **Jonathan A. Jones a Michele Mosca** implementují Deutschův-Jozsovův algoritmus (2 qubity)
- 1997: **první kvantová teleportace** (Innsbruck)



Nature **390**, 575 (1997)

první desetiletí 21. století

- 2001: IBM faktorizuje číslo 15 (Shorův algoritmus)

.....

Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance

Lieven M. K. Vandersypen^{*†}, Matthias Steffen^{*†}, Gregory Breyta^{*}, Costantino S. Yannoni^{*}, Mark H. Sherwood^{*} & Isaac L. Chuang^{*†}

^{*} IBM Almaden Research Center, San Jose, California 95120, USA

[†] Solid State and Photonics Laboratory, Stanford University, Stanford, California 94305-4075, USA

Nature **414**, 883 (2001)

- 2001: **IBM** faktorizuje číslo 15 (Shorův algoritmus)
- pokračuje experimentální výzkum – přicházejí nové platformy (například **supravodivé qubity**)

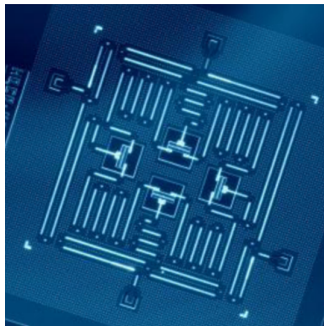


Foto: IBM

- 2001: **IBM** faktorizuje číslo 15 (Shorův algoritmus)
- pokračuje experimentální výzkum – přicházejí nové platformy (například **supravodivé qubity**)
- 2007: **D-Wave** ohlašuje první kvantový počítač (28 qubitů)

D-WAVE
The Quantum Computing Company™



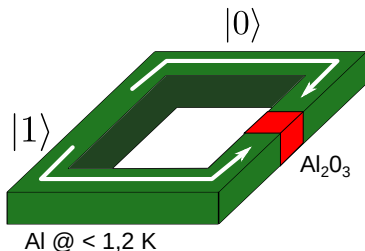
Kvantové počítače dnes

Foto: techpinions.com

Supravodivé qubity

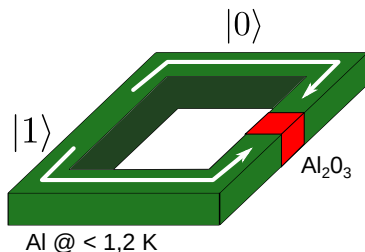
Supravodivé qubity

- prstence ze supravodivého materiálu mikrometrických rozměrů



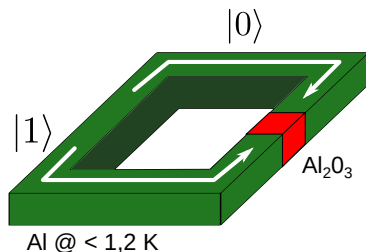
Supravodivé qubity

- prstence ze supravodivého materiálu mikrometrických rozměrů
- elektrony při velmi nízké teplotě ztrácí odpor



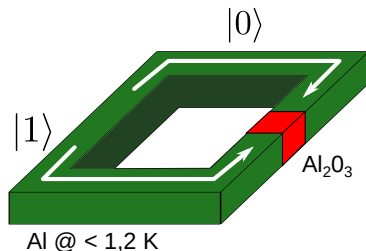
Supravodivé qubity

- prstence ze supravodivého materiálu mikrometrických rozměrů
- elektrony při velmi nízké teplotě ztrácí odpor
- proud může téci ve směru i proti směru hodinových ručiček



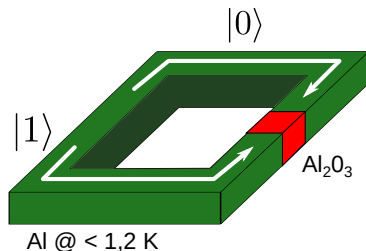
Supravodivé qubity

- prstence ze supravodivého materiálu mikrometrických rozměrů
- elektrony při velmi nízké teplotě ztrácí odpor
- proud může téci ve směru i proti směru hodinových ručiček
- stav lze manipulovat vnějším elektromagnetickým polem



Supravodivé qubity

- prstence ze supravodivého materiálu mikrometrických rozměrů
- elektrony při velmi nízké teplotě ztrácí odpor
- proud může téci ve směru i proti směru hodinových ručiček
- stav lze manipulovat vnějším elektromagnetickým polem
- *pozn.: existují i jiné metody zápisu qubitu v supravodivém obvodu*



D-Wave



- 2011: první **komerční** kvantový počítač **D-Wave One** (128 qubitů)

- 2011: první **komerční** kvantový počítač **D-Wave One** (128 qubitů)
- 2013: rozšíření na 512 qubitů – **D-Wave Two**

- 2011: první **komerční** kvantový počítač **D-Wave One** (128 qubitů)
- 2013: rozšíření na 512 qubitů – **D-Wave Two**
- 2015: rozšíření na 1152 qubitů – **D-Wave 2X**

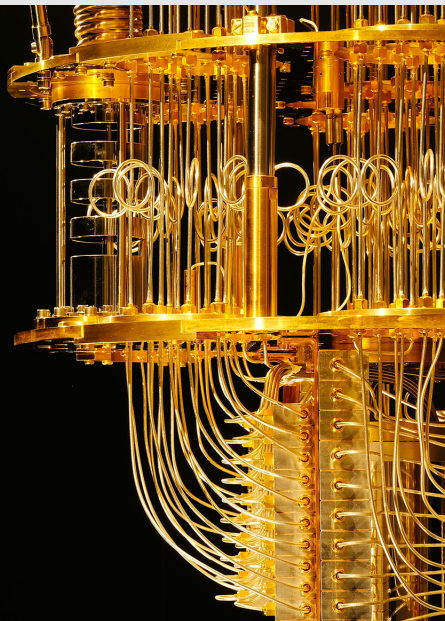
- 2011: první **komerční** kvantový počítač **D-Wave One** (128 qubitů)
- 2013: rozšíření na 512 qubitů – **D-Wave Two**
- 2015: rozšíření na 1152 qubitů – **D-Wave 2X**
- 2017: rozšíření na 2048 qubitů – **D-Wave 2000Q**

- 2011: první **komerční** kvantový počítač **D-Wave One** (128 qubitů)
- 2013: rozšíření na 512 qubitů – **D-Wave Two**
- 2015: rozšíření na 1152 qubitů – **D-Wave 2X**
- 2017: rozšíření na 2048 qubitů – **D-Wave 2000Q**
- 2020: plán na 5000 qubitů

- nejedná se ale o univerzální počítač

- nejedná se ale o **univerzální počítač**
- schopen řešit pouze jeden typ úlohy: **hledání minima složité funkce**

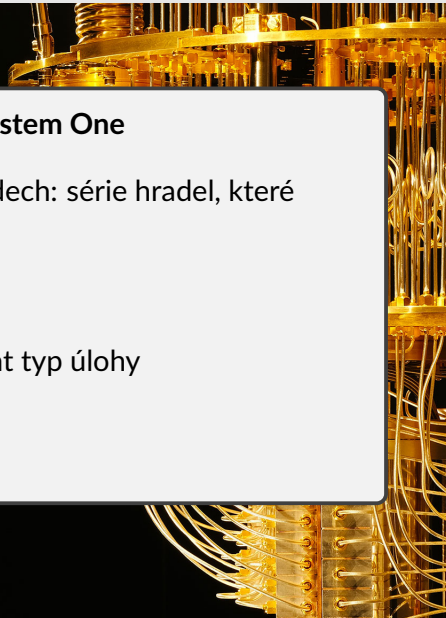
- nejedná se ale o **univerzální počítač**
- schopen řešit pouze jeden typ úlohy: **hledání minima složité funkce**
- doprovázený klasickými procesory, které úlohu přechystají



- 2019: první komerční verze **System One**

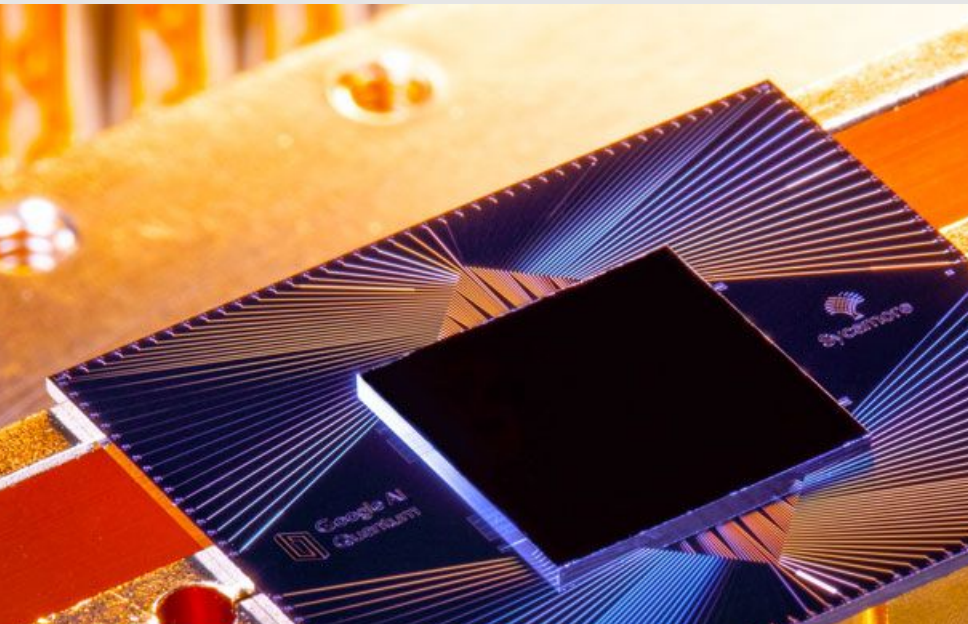
- 2019: první komerční verze **System One**
- první řešení založené na obvodech: série hradel, které mají být postupně vykonány

- 2019: první komerční verze **System One**
- první řešení založené na obvodech: série hradel, které mají být postupně vykonány
- blíží se **univerzálnímu počítači**

- 
- 2019: první komerční verze **System One**
 - první řešení založené na obvodech: série hradel, které mají být postupně vykonány
 - blíží se **univerzálnímu počítači**
 - oproti D-Wave lze programovat typ úlohy

- 2019: první komerční verze **System One**
- první řešení založené na obvodech: série hradel, které mají být postupně vykonány
- blíží se **univerzálnímu počítači**
- oproti D-Wave lze programovat typ úlohy
- není univerzální (nelze aplikovat hradlo CNOT mezi libovolné páry qubitů) a má relativně málo qubitů (53)

Google Sycamore



- doposud klasické počítače držely s kvantovými krok

- doposud klasické počítače držely s kvantovými krok
- 2019: první **reálné a podstatné zrychlení**

- doposud klasické počítače držely s kvantovými krok
- 2019: první **reálné a podstatné** zrychlení
- jeden výpočet trval **Sycamoru** 200 s

- doposud klasické počítače držely s kvantovými krok
- 2019: první **reálné a podstatné zrychlení**
- jeden výpočet trval **Sycamoru** 200 s
- klasický superpočítač by potřebovat 10 000 let

- doposud klasické počítače držely s kvantovými krok
- 2019: první **reálné a podstatné zrychlení**
- jeden výpočet trval **Sycamoru** 200 s
- klasický superpočítač by potřebovat 10 000 let
- problém: velmi specifická úloha (simulace kvantového obvodu)

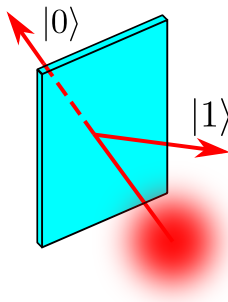
- doposud klasické počítače držely s kvantovými krok
- 2019: první **reálné a podstatné zrychlení**
- jeden výpočet trval **Sycamoru** 200 s
- klasický superpočítač by potřebovat 10 000 let
- problém: velmi specifická úloha (simulace kvantového obvodu)
- Sycamore má 54 qubitů a opět není zcela univerzální

Jára Cimrman:
Zkuste to bez drátů, milý Marconi!

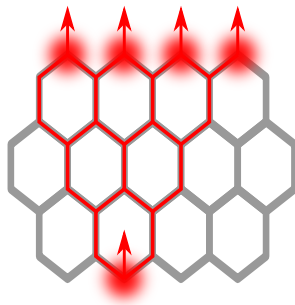
Fotonické qubity

- **jeden foton** nese pozorovatelnou dávku energie, lze detekovat

- **jeden foton** nese pozorovatelnou dávku energie, lze detekovat
- foton na polopropustném zrcátku: nerozdělí se na dva, ale **projde i se odrazí naráz** (superpozice drah)



- **jeden foton** nese pozorovatelnou dávku energie, lze detekovat
- foton na polopropustném zrcátku: nerozdělí se na dva, ale **projde i se odrazí naráz** (superpozice drah)
- z optických vláken lze sestavit složitá zařízení – **interferometry** – ve kterých se vyvíjí kvantový svět světla



Počítání se světlem

- jednoúčelové algoritmy, zpravidla pro **kvantové strojové učení**

- jednoúčelové algoritmy, zpravidla pro **kvantové strojové učení**
- složité interferometry jsou vyvíjeny pomocí **integrované optiky**

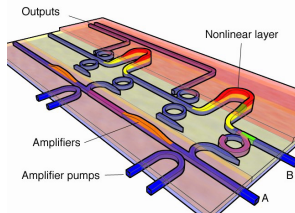
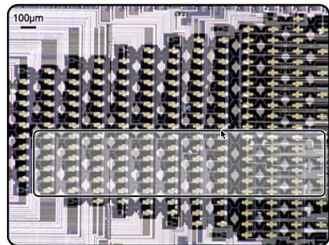


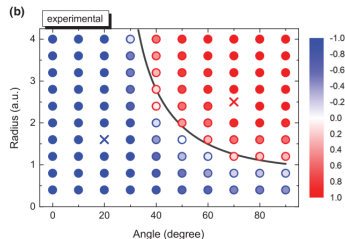
Foto: Liberal dictionary

- jednoúčelové algoritmy, zpravidla pro **kvantové strojové učení**
- složité interferometry jsou vyvíjeny pomocí **integrované optiky**
- neuronové sítě



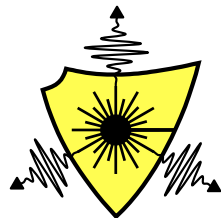
Nat. Photon. **11**, 441 (2017)

- jednoúčelové algoritmy, zpravidla pro **kvantové strojové učení**
- složité interferometry jsou vyvíjeny pomocí **integrované optiky**
- neuronové sítě
- klasifikační algoritmy



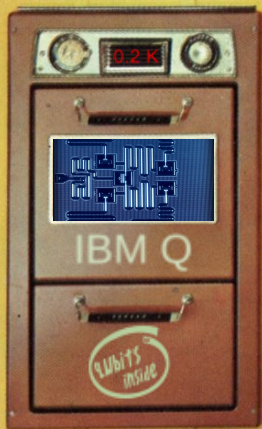
Phys. Rev. Lett. **114**, 110504 (2015)

- jednoúčelové algoritmy, zpravidla pro **kvantové strojové učení**
- složité interferometry jsou vyvíjeny pomocí **integrované optiky**
- neuronové sítě
- klasifikační algoritmy
- málo šumu, není třeba chlazení, ne každá úloha je ale vhodná pro světlo
→ **naš výzkum**



VÍCEFOTONOVÁ
KVANTOVÁ
LABORATOŘ

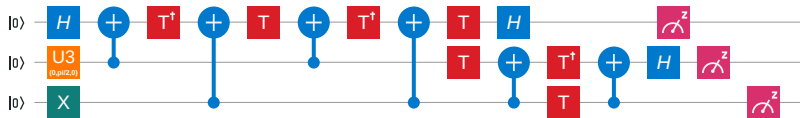
UNIVERZITA PALACKÉHO



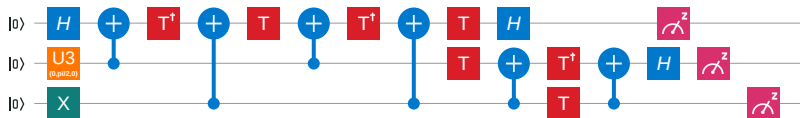
Kvantový počítač do každé domácnosti

- **zdarma** výpočetní čas na kvantových procesorech

- **zdarma** výpočetní čas na kvantových procesorech
- pro začátečníky: **skladatel** – grafické skládání kvantových obvodů



- **zdarma** výpočetní čas na kvantových procesorech
- pro začátečníky: **skladatel** – grafické skládání kvantových obvodů

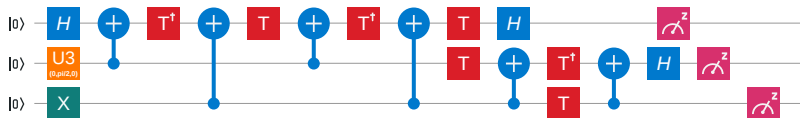


- pro pokročilé: **QISKIT** – knihovna pro Python umožňující programování kvantových procesorů

```
for b in IBMQ.backends():  
    >> selected = ""  
    >> if (b.name() == processor):  
    >> selected = " <--- selected"
```

IBM Quantum Experience

- **zdarma** výpočetní čas na kvantových procesorech
- pro začátečníky: **skladatel** – grafické skládání kvantových obvodů



- pro pokročilé: **QISKIT** – knihovna pro Python umožňující programování kvantových procesorů

```
for b in IBMQ.backends():  
    >> selected = ""  
    >> if (b.name() == processor):  
    >> selected = " <--- selected"
```

- <https://quantum-computing.ibm.com/>

IBM Quantum Experience (<https://quantum-computing.ibm.com/>)

New Save Clear Delete Help

GHZ_Hardy

Saved

Run



Composer help



The circuit composer is a tool that allows you to visually learn how to create quantum circuits. Here are some resources to get you started.

[Composer guide](#)

[Gates overview](#)

Circuit composer

[Gates overview](#)

Gates



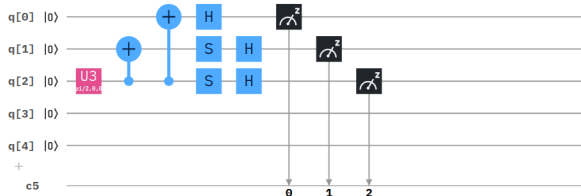
Barrier

Operations

Subroutines



+ Add



A person is seen from behind, floating in a calm body of water. The water reflects the person and the surrounding landscape. In the background, there are lush green hills and mountains under a clear sky. The overall scene is peaceful and scenic.

Výhled

Foto: pexels.com

- v dohledné době kvantové počítače **nenahradí** ty klasické

- v dohledné době kvantové počítače **nenahradí** ty klasické

Důvody:

- náročné na provoz (chlazení pod 2 K)
- chybí kvantový Internet a dobré paměti
- vyplatí se pouze na specifické úlohy
- ne vždy zrychlení oproti klasickým algoritmům

- v dohledné době kvantové počítače **nenahradí** ty klasické

Důvody:

- náročné na provoz (chlazení pod 2 K)
- chybí kvantový Internet a dobré paměti
- vyplatí se pouze na specifické úlohy
- ne vždy zrychlení oproti klasickým algoritmům

Uplatnění:

- **syntéza** s klasickým počítačem
- specifické výpočty, kde kvantový algoritmus dává zrychlení
- zatím velké korporace nebo vzdálený přístup
- časem možné rozšíření
- **hrozba pro klasickou kryptografii**

- klasická kryptografie spoléhá na velkou výpočetní náročnost útoku

- klasická kryptografie spoléhá na velkou výpočetní náročnost útoku
- **asymetrická šifra** (nejčastěji RSA) – obtížnost faktorizace součinu prvočísel – lze zaútočit Shorovým algoritmem

- klasická kryptografie spoléhá na velkou výpočetní náročnost útoku
- **asymetrická šifra** (nejčastěji RSA) – obtížnost faktorizace součinu prvočísel – lze zaútočit Shorovým algoritmem
- **symetrická šifra** – lze zaútočit Groverovým algoritmem a rychleji najít řešení

- klasická kryptografie spoléhá na velkou výpočetní náročnost útoku
- **asymetrická šifra** (nejčastěji RSA) – obtížnost faktorizace součinu prvočísel – lze zaútočit Shorovým algoritmem
- **symetrická šifra** – lze zaútočit Groverovým algoritmem a rychleji najít řešení

Řešení:

- klasická kryptografie spoléhá na velkou výpočetní náročnost útoku
- **asymetrická šifra** (nejčastěji RSA) – obtížnost faktorizace součinu prvočísel – lze zaútočit Shorovým algoritmem
- **symetrická šifra** – lze zaútočit Groverovým algoritmem a rychleji najít řešení

Řešení:

- zcela nekoncepční: zvýšit délku klíče a doufat

- klasická kryptografie spoléhá na velkou výpočetní náročnost útoku
- **asymetrická šifra** (nejčastěji RSA) – obtížnost faktorizace součinu prvočísel – lze zaútočit Shorovým algoritmem
- **symetrická šifra** – lze zaútočit Groverovým algoritmem a rychleji najít řešení

Řešení:

- zcela nekoncepční: zvýšit délku klíče a doufat
- napůl nekoncepční: nahradit šifry **postkvantovou kryptografií** – klasická kryptografie založená na úlohách, u kterých neznáme rychlý kvantový algoritmus, a doufat

- klasická kryptografie spoléhá na velkou výpočetní náročnost útoku
- **asymetrická šifra** (nejčastěji RSA) – obtížnost faktorizace součinu prvočísel – lze zaútočit Shorovým algoritmem
- **symetrická šifra** – lze zaútočit Groverovým algoritmem a rychleji najít řešení

Řešení:

- zcela nekoncepční: zvýšit délku klíče a doufat
- napůl nekoncepční: nahradit šifry **postkvantovou kryptografií** – klasická kryptografie založená na úlohách, u kterých neznáme rychlý kvantový algoritmus, a doufat
- koncepční: **kvantová kryptografie** – o bezpečnost se starají přírodní zákony a ne pouze víra ve příliš velkou výpočetní náročnost prolomení

- klasická kryptografie spoléhá na velkou výpočetní náročnost útoku
- **asymetrická šifra** (nejčastěji RSA) – obtížnost faktorizace součinu prvočísel – lze zaútočit Shorovým algoritmem
- **symetrická šifra** – lze zaútočit Groverovým algoritmem a rychleji najít řešení

Řešení:

- zcela nekoncepční: zvýšit délku klíče a doufat
- napůl nekoncepční: nahradit šifry **postkvantovou kryptografií** – klasická kryptografie založená na úlohách, u kterých neznáme rychlý kvantový algoritmus, a doufat
- koncepční: **kvantová kryptografie** – o bezpečnost se starají přírodní zákony a ne pouze víra ve příliš velkou výpočetní náročnost prolomení
- výzkum od roku 1984 a stále pokračuje

Děkuji za pozornost

Dny otevřených dveří, exkurze do laboratoře,
novinky z našeho výzkumu:

